The Top Malware Families in Banking, Mobile, Ransomware, and Crypto-Mining of 2017

DAVID BISSON (HTTPS://WWW.TRIPWIRE.COM/STATE-OF-SECURITY/CONTRIBUTORS/DAVID-BISSON/) Follow @DMBisson

JAN 30, 2018 | FEATURED ARTICLES (/STATE-OF-SECURITY/TOPICS/FEATURED/)

(HTTPS://WWW.TRIPWIRE.COM/STATE-

41

The second half of 2017 was busy in terms of digital security events. In September, consumer reporting agency Equifax announced a breach (https://www.tripwire.com/state-of-security/latest-security-news/equifax-data-breach-impact-143-million-consumers/) that potentially compromised the Social Security Numbers and other personal information of 143 million U.S. consumers.

Less than two months later, organizations in Russia and Ukraine suffered infections at the hands of BadRabbit (https://www.tripwire.com/state-of-security/featured/badrabbit-runs-steam-prepared-next-ransomware-attack/), the third international ransomware outbreak of the year. 2017 ended with Check Point's announcement (https://www.tripwire.com/state-of-security/latest-security-news/crypto-miner-named-wanted-malware-december-2017/) that a cryptocurrency miner had, for the first time, topped its monthly Global Threat Index.

These are just some of the security incidents that shaped H2 2017. To get a more comprehensive view of those six months, Check Point drew data from its ThreatCloud collaborative intelligence network to produce the *H2 2017 Global Threat Intelligence Trends Report (https://research.checkpoint.com/h2-2017-global-threat-intelligence-trends-report)*.

This report synthesizes information yielded from 250 million addresses analyzed for bot discovery, 11 million malware signatures, and 5.5 million infected websites to shed light on some of the most prevalent malware families and other digital threats that defined the second half of the year.

Here are some of the report's major findings.

Global Trends

Several notable trends emerged from Check Point's ThreatCloud data collected during the second half of 2017. One of the most significant developments was the rise of cryptocurrency miners. Maya Horowitz, threat intelligence group manager at Check Point, comments on this movement:

The second half of 2017 has seen crypto-miners take the world by storm to become a favorite monetizing attack vector. While this is not an entirely new malware type, the increasing popularity and value of cryptocurrency has led to a significant increase in the distribution of crypto-mining malware.

Indeed, what made cryptocurrency miners stand out in H2 2017 was the injection of these tools (knowingly or unknowingly) into websites without notifying users. Some organizations might have embraced this practice to replace web advertisements in the age of ad-blockers. In so doing, however, they oftentimes consumed more than half of the CPU on unsuspecting visitors' machines. Check Point estimates that one in five organizations were victims (or adopters) of cryptocurrency miner injection in December 2017.

While cryptocurrency miners surged over the course of the second half of the year, exploit kits decreased in use. Various factors drove this decline, including new security mechanisms introduced by web browsers and the increasing difficulty of discovering zero-day vulnerabilities before they're sold on the dark web. Many exploit kits therefore resorted to using older security flaws already patched by software vendors, a response which decreased both the number of drive-by attacks and the development of new kits.

Cryptocurrency minders weren't the only digital threat to have a better six months than exploit kits. So too did spam operations and malspam. Indeed, 62% of infections leveraged SMTP in H2 2017, which paved the way for more skilled threat actors using high-quality campaigns consisting of new vulnerabilities and file types like .xlam and .xlb.

Here's a breakdown of malicious file type activity in the second half of the year:

Check Point's *H2 2017 Global Threat Intelligence Trends Report* page 5

Last but not least, multiple malware families emerged in H2 2017 that reuse code from already successful digital threats. For example, two Internet of Things (IoT) botnets called IoTroop and Satori borrowed code from Mirai (https://www.tripwire.com/state-of-security/featured/mirai-botnet-three-men-plead-guilty-weaponizing-internet-things/) to stake their claim in the digital threat landscape. IoTroop, in particular, uses vulnerability scanning instead of Mirai's brute force password cracker to compromise vulnerable smart devices.

The Most Prevalent Families

Check Point's report also reveals the most prevalent malware families in several different categories. Those rankings are presented below:

TOP MALWARE FAMILIES (OVERALL)

1. **Roughted (15.3%)** – A large-scale malvertising campaign that spiked in May and peaked in June, affecting organizations located in over 150 countries. The threat fell by a third from 28% of all corporate networks affected to just 18% a month later.
2. **CoinHive (8.3%)** – A crypto-miner of Monero cryptocurrency. CoinHive launched in September 2017 but quickly grew in popularity, becoming the "most wanted" malware on Check Point's Global Threat Index for December 2017.
3. **Locky (7.9%)** – A crypto-ransomware family that first emerged in February 2016. It's since climbed back to into the top malware ranks after dropping in H1 2017.

TOP RANSOMWARE FAMILIES

1. **Locky (30%)** – It spreads mainly via spam emails containing a downloader that's disguised as a Word or Zip attachment. The downloader, in turn, drops Locky crypto-malware that encrypts the user files.
2. **Globeimposter (26%)** – A ransomware family that first emerged in May 2017. It relies on spam campaigns, malvertising, and exploit kits for distribution. Upon encryption, the threat appends the .crypt extension to each encrypted file.
3. **WannaCry (15%)** – Ransomware that enjoyed a global outbreak in May 2017. It spreads by exploiting a Windows SMB vulnerability, allowing it to move laterally within and between corporate networks.

Check Point's *H2 2017 Global Threat Intelligence Trends Report* page 13

TOP BANKING MALWARE FAMILIES

1. **Ramnit (34%) –** A trojan that steals banking credentials, FTP passwords, session cookies, and personal data.
2. **Zeus (22%)** – Malware that targets Windows platforms and steals banking information via man-in-the-browser keystroke logging and form grabbing.
3. **Tinba (16%)** – A threat that steals victims' credentials using web-injects that are activated as the user attempts to log in to their account on their bank's website.

TOP MOBILE MALWARE FAMILIES

1. **Hidad (55%)**– Android malware that repackages legitimate apps in order to display ads and releases them to a third-party store. It gains access to key security details built into the OS and thereby obtains sensitive user data.
2. **Triada (8%)**– A modular Android backdoor that grants super-user privileges to downloaded malware and helps samples embed themselves into system processes. This threat has also been seen spoofing URLs loaded in the browser.
3. **Lotoor (8%)**– A hacking tool that exploits vulnerabilities in Android OS so that it can achieve root privileges.

TOP CRYPTO-MINING MALWARE

1. **CoinHive (52%)** – CoinHive is a JavaScript cryptocurrency miner that website owners can embed into their site. It then mines for Monero without a site visitor's knowledge.
2. **Cryptoloot (13%)** – Another JavaScript miner that functions similarly to CoinHive. In fact, bad actors commonly market Cryptoloot as a CoinHive alternative.

3. **Coinnebula (8%)** – Microsoft observed this in-browser miner in several video-streaming websites back in October 2017.

Predictions for 2018

Looking ahead to 2018, Check Point has several predictions. First, it estimates that blockchain attacks will evolve. It anticipates the security industry will see new methods of conducting virtual wallet and credential theft as well as cryptocurrency transaction theft. The security firm also predicts banking trojans capable of collecting virtual wallet credentials will become more commonplace; it feels the same will occur for digital attackers using mobile botnets to mine for cryptocurrencies illicitly.

Second, Check Point predicts that more sophisticated IoT attack types will emerge. More prolific IoT zero-day vulnerability research will lead to underground markets that can in part help spawn new attack types and new ways to leverage infected devices and collected data. For example, the company suspects that attackers will devise methods that target specific devices, thereby potentially leading to more breaches and extortion.

Finally, Check Point anticipates that the security industry will see more cross-platform malware attacks, such as ransomware that's capable of encrypting a hospital's network, employees' mobile phones, and all web-connected medical equipment.

Facing Future Threats Together

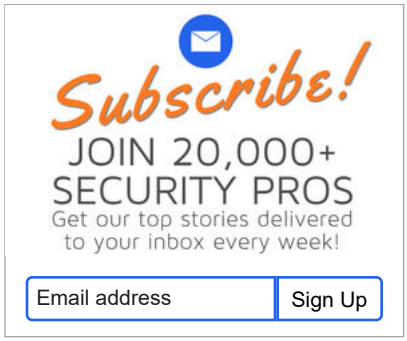
Check Point's *H2 2017 Global Threat Intelligence Trends Report* clearly demonstrates the importance of threat intelligence. Organizations can use this information to educate their users and to better defend against digital threats. That is especially the case when companies like Tripwire and Check Point form partnerships to better protect their customers.

Jim Wichhaus, Director of Tripwire's Technology Alliance Program (TAP), is well aware of the advantage that technology partnerships exercise against digital threats:

> *Because mature organizations seek the best reliability, protection, and compliance, we deem it critical to Tripwire's mission and to yours to partner and integrate with leading industrial & IT cybersecurity software and hardware providers. Most organizations are adopting frameworks as a roadmap and applying critical controls first to the cybersecurity problem. And while this generates almost immediate and ongoing ROI, we still face technical roadblocks to integration and automation, especially when it's a given that expertise is difficult to find and fund. Partnerships help remove these roadblocks so you can build your cybersecurity effectiveness and efficiency on Tripwire's foundational controls (https://www.tripwire.com/products/tripwire-enterprise/).*

To learn more about Tripwire's Technology Alliance Program, please click here (https://www.tripwire.com/partners/tap-partners/).

41



(https://www.tripwire.com/solutions/configure-and-harden-your-systems/security-configuration-management-for-dummies-book-register/?utm_source=sos&utm_medium=sb-bnr&utm_content=pdf&utm_campaign=scm-for-dummies)

(https://www.tripwire.com/solutions/configure-and-harden-your-systems/sans-back-to-basics-register/)

TOPICS

ICS Security (/state-of-security/topics/ics-security/)
Incident Detection (/state-of-security/topics/incident-detection/)
IT Security and Data Protection (/state-of-security/topics/security-data-protection/)
Latest Security News (/state-of-security/topics/tripwire-news/)
Regulatory Compliance (/state-of-security/topics/regulatory-compliance/)
Security Awareness (/state-of-security/topics/security-awareness/)
Vulnerability Management (/state-of-security/topics/vulnerability-management/)

ABOUT

About (/state-of-security/about/)
Contributors (/state-of-security/contributors/)
Write for us (/state-of-security/about/contact-us/)
Privacy Policy (/legal/privacy/)
Tripwire.com (/)

CONTACT US

US Headquarters
101 SW Main St., Ste. 1500
Portland, OR 97204
(https://www.google.com/maps/place/One+Main+Place,+101+SW+Main+St+%231500,+Portland,+OR+97204/@45.5155036,-122.6775251,17z/data=!3m1!4b1!4m5!3m4!1s0x54950a0fb0d
122.6753364)

Direct: 503.276.7500 (tel:5032767500)

International Offices (/contact/)

SEARCH